EGI-CSIRT Operational Security

Vincent Brillault, for the EGI IRTF

EGI-Engage is co-funded by the Horizon 2020 Framework Programme
of the European Union under grant number 654142

Recent Incidents

Incidents

- EGI-20200219-001 . . . OpenSSH trojan on accademic systems
- EGI-20200422-01 Security incident at CA-. . .

Monitoring

Monitoring

- Monitoring is checking availability:
  - Checking if service is up
  - Checking if ACLs are open enough
  - Not validating if they are too open!

  $\rightarrow$ Can be tempting to disable ACLs for availability
- Following a report from a user, ACLs were checked with writing atlas storage using dteam proxy
  - 7 cases followed up directly
  - 1 case still open: testing with ATLAS

Communication Challenge

Communication Challenge
How it works

- Same process as in 2018 (should be annual...)
- Contacting every site security contact by mail
  - Through the same tool(s) we used for IR
- Asking to click on a link (no privilege required)
- Following up sites who do not click

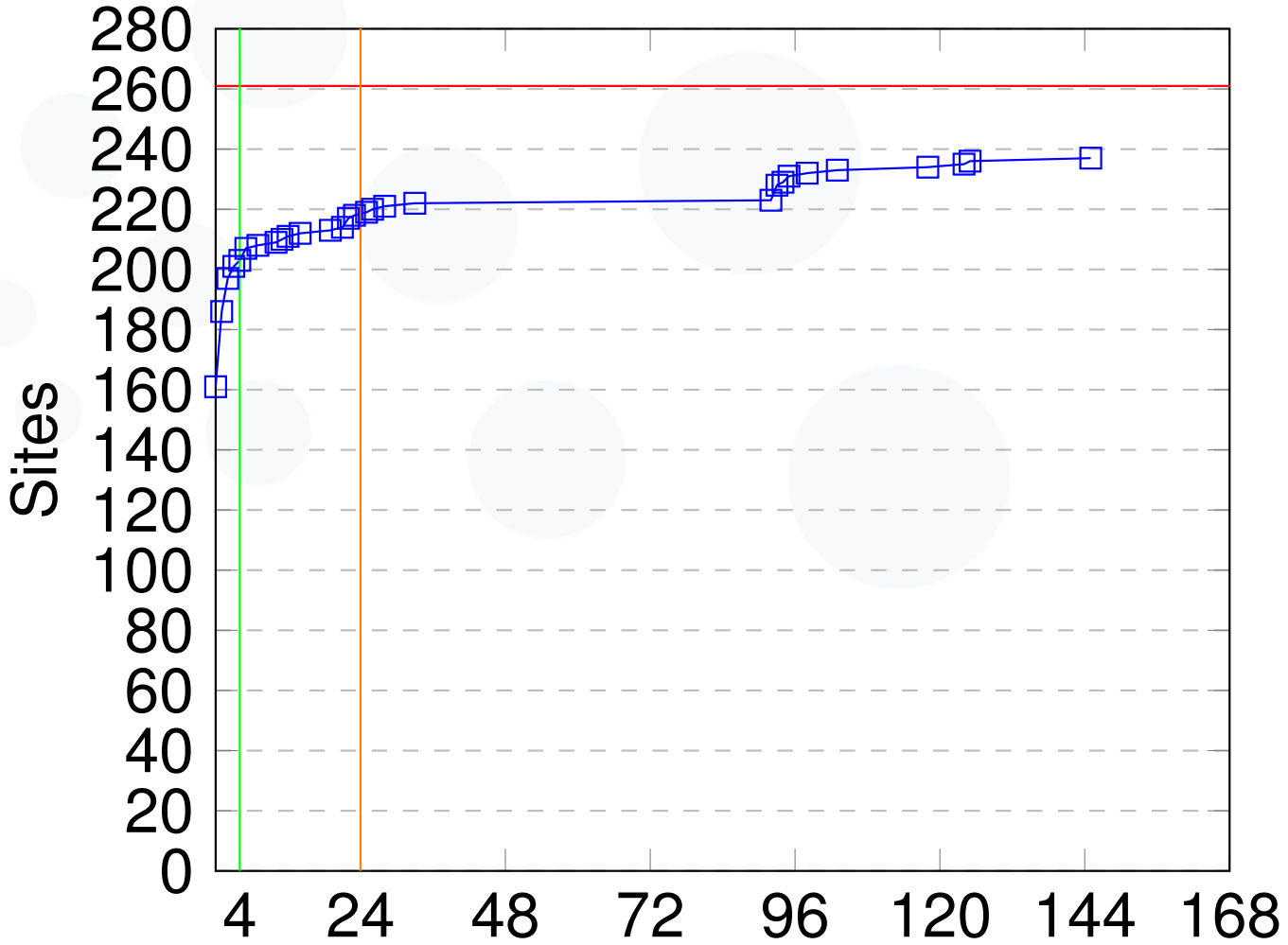
Communication Challenge Timeline

- Prepared in the last month (checking & fixing tools)
- Started on 2020-04-16 around lunch time
- Reminder sent on 2020-04-20 in the morning

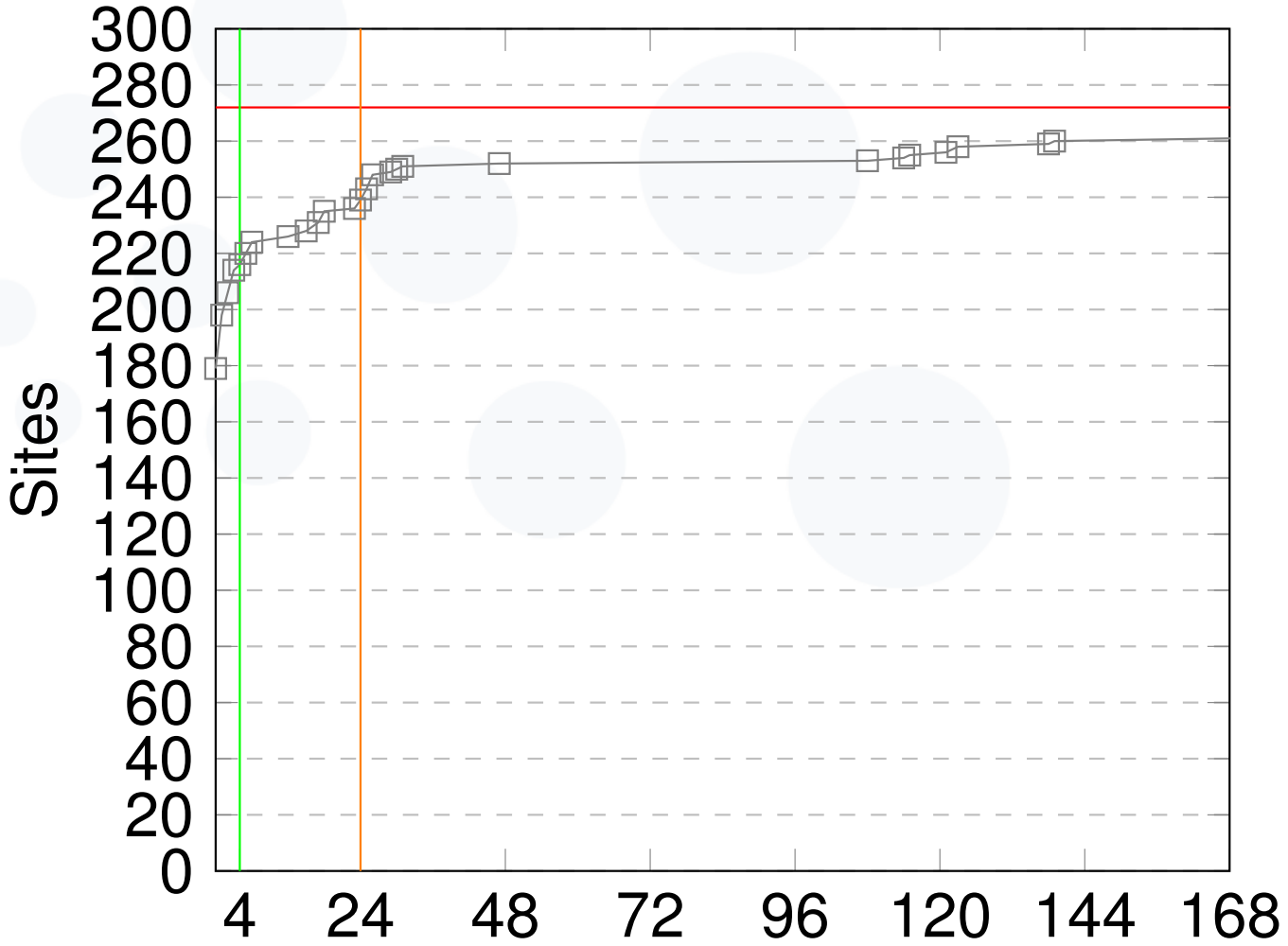
Communication Challenge Results

- As of 08:45 this morning: 237/261 clicked
- Few problems already identified:
  - One site without security contact: fixed
  - One site with outdated security contact: fixed
  - 3 sites with mail issues: being followed up

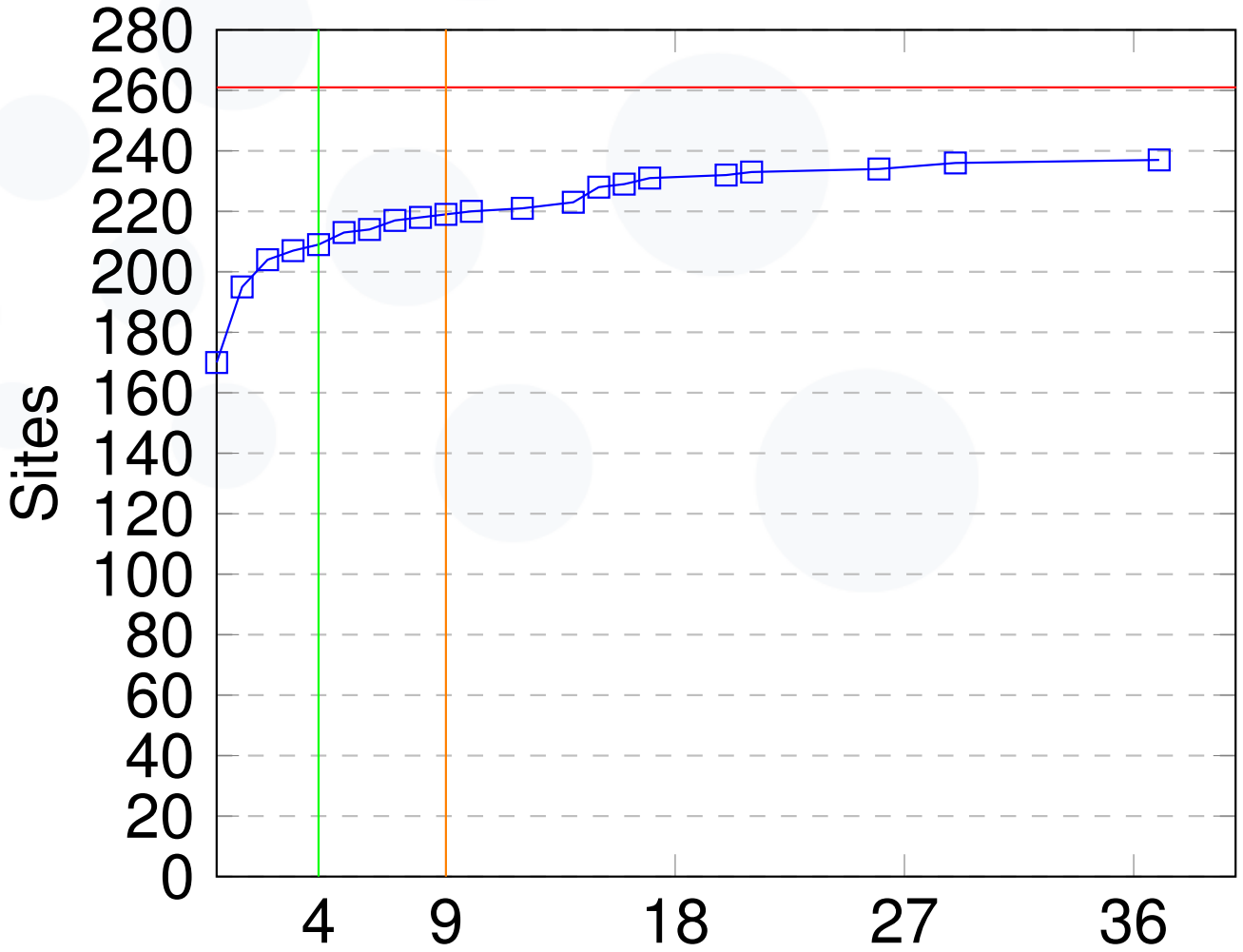
Communication Challenge
Time to click in hours (raw)



Communication Challenge
Time to click in hours (raw)
Last campaign (2018)



Communication Challenge Time to click in working hours (8:30 to 17:30 in site timezone)



Communication Challenge Next step

- Contact NGI security contacts to check remaining:
  - AFRICAARABIA 1
  - ASIAPACIFIC 1
  - EGI.EU 5
  - NGI_CH 1
  - NGI_DE 1
  - NGI_FI 5
  - NGI_RO 1
  - NGI_UK 2
  - ROC_CANADA 4
  - ROC_LA 2
  - RUSSIA 1

Communication Challenge
Next Challenge

- In the coming weeks: same exercise for VOs!
  - Due to pilot jobs & VO framework, VOs are part of IR
- Same process & tools as for sites
- First time: let's see how it goes!

Any question?